HW 8

When I refer to specific theorem numbers, they're from the book “Elementary Number Theory” by Jones and Jones, published by Springer. I sometimes use the shorthand CRT for the Chinese Remainder Theorem. I use the notation \( \mathbb{Z}_n \) for the integers mod \( n \), and \( U_n = (\mathbb{Z}_n)^* \) for the group of units. Please let me know if there are any typos or mistakes by emailing arjun-at-cims-dot-nyu-dot-edu.

Problem 1.

Part (a): \( n = 43^5 \cdot 29^6 = n_1n_2 \). Since \( n \) is odd, we can multiply the quadratic by 4, and factorize as usual to get

\[
4(x^2 + 5x + 8) = (2x + 5)^2 - 25 + 32 = y^2 = -7 \mod n_1n_2,
\]

where \( y = 2x + 5 \). We can solve this equation for \( y \) iff \(-7\) is a quadratic residue mod \( 43^5 \) and mod \( 29^6 \). We know that \(-7\) is a quadratic residue mod an odd prime power \( p^e \) iff it is a quadratic residue mod \( p \); both \( n_1 \) and \( n_2 \) are odd prime powers.

So it’s enough to compute \( \left( \frac{-7}{43} \right) \) and \( \left( \frac{-7}{29} \right) \) and ensure that they’re both 1:

\[
\left( \frac{-7}{43} \right) = \left( \frac{-1}{43} \right) \left( \frac{43}{7} \right) = (-1) \left( -1 \right) \left( \frac{1}{7} \right) = 1.
\]

Here we’ve used quadratic reciprocity for \( \left( \frac{43}{7} \right) \), and the fact that \(-1 \in \mathbb{Q}_p \) iff \( p = 1 \mod 4 \).

Similarly,

\[
\left( \frac{-7}{29} \right) = 1 \cdot \left( \frac{29}{7} \right) = 1.
\]

When \( p \) is an odd prime, there is a primitive root in \( U_{p^e} \). Then, the number of solutions to \( y^2 = -7 \mod p^e \), if they exist at all, is 2. Therefore, there are a total for \( 2 \cdot 2 = 4 \) solutions to \( y^2 = -7 \mod n_1n_2 \). Since both \( n_1 \) and \( n_2 \) are odd, 2 is coprime to both of them. Hence, \( 2x + 5 = y \mod n_i \) has one solution for each \( y \). This gives a total of 4 solutions. You can always check your solutions on a computer. Example:

- **WolframAlpha command:** solve \( x^2 + 5x + 8 \) Mod \( 43^5 \cdot 29^6 = 0 \)
- **Mathematica command:** Solve\( [x^2 + 5x + 8 = 0, \text{Modulus} -> 43^5 \cdot 29^6] \)

Part (b): First, notice that \( x^2 + 5x + 4 = 0 \mod 2^{500} \) can be factorized as

\[
(x + 1)(x + 4) = 0 \mod 2^{500}.
\]

From this it follows that \( x = -1 \) and \( x = -4 \) are solutions. Are these the only solutions?

We could solve this problem as we did in part (a) by multiplying the equation by 4 and completing the square. However, 4 is not coprime to \( 2^{500} \), and we must account this by changing the modulus:

\[
2^2 f(x) = 0 \mod 2^{e+2},
\]
where \( f(x) = x^2 + 5x + 1 \) and \( e = 500 \). However, a moment’s thought tells us that
\[
2^2 f(x) = 0 \mod 2^{e+2} \iff f(x) = 0 \mod 2^e,
\]
where \( x \in \mathbb{Z} \) (think about the congruences in terms of divisibility). This tells us that the integers solving both congruences are the same. Now, let’s look at equivalence classes of solutions mod \( 2^e \) and \( 2^{e+2} \). Because of the one-one correspondence between solutions, it follows that there are \( k \) solutions mod \( 2^e \) iff there are \( 4k \) solutions mod \( 2^{e+2} \). This is because there are 4 copies of the group \( 2^e \) in \( 2^{e+2} \).

Completing the square, we get
\[
(2x + 5)^2 = 9 \mod 2^{e+2}
\]
Make the substitution \( y = 2x + 5 \) to get \( y^2 = 9 \mod 2^{e+2} \). We know that \( 9 \in Q_{2^{e+2}} \) since \( 3^2 = 9 \). Our theory also tells us that there are four square roots in \( U_{2^{e+2}} \) for each member of \( Q_{2^{e+2}} \). You can rederive this result yourself by recalling that \( U_{2^e} = \{ \pm 5^i \mid 0 \leq i \leq 2^{e-2} \} \) for \( e \geq 3 \). Each square root \( y \) is in \( U_{2^e} \), and hence \( y - 5 \) is even. Then, we can write
\[
x = \frac{y - 5}{2} \mod 2^{e+1}.
\]
Hence, for each of the four square root \( y \), there are two solutions for \( x \in Z_{2^{e+2}} \). This gives us a total of 8 solutions for \( x \). We noted earlier that if there are 8 solutions mod \( 2^{e+2} \), there must be \( 8/4 = 2 \) solutions mod \( 2^e \). This is the final answer.

There is a much simpler way to solve this using lifting. Recall Hensel’s lemma: let \( f(x) \) be a polynomial and let \( p \) be prime. Suppose there is a \( r \in \mathbb{Z} \) s.t.
\[
f(r) = 0 \mod p \text{ and } f'(r) \neq 0.
\]
Then, for each \( e > 1 \), there is a unique \( s \in \mathbb{Z}_p^* \) such that
\[
f(s) = 0 \mod p^e \text{ and } r = s \mod p.
\]
Here, \( f(x) = x^2 + x \mod 2 \) has both 0 and 1 as solutions. \( f'(x) = 2x + 5 = 1 \mod p \). So both 0 and 1 lift uniquely to roots of \( f(x) = 0 \mod 2^e \) for all \( e > 1 \). In other words, there are exactly two roots mod \( 2^e \) for all \( e: -1 \) and \(-4\).

**Part (c):** I’m going to assume that the intended equation was \( x^2 + 2px + 1 \). Otherwise the problem reduces to finding when \(-1\) is a quadratic residue mod \( p \), which we know how to solve. We can easily factorize the quadratic as
\[
x^2 + 2px + 1 = (x + p)^2 - (p + 1)(p - 1).
\]
Set \( x + p = y \), and note that both \( (p + 1) \) and \( (p - 1) \) \( \in U_{p^e} \). Hence, we only need to determine if \( (p + 1)(p - 1) \) is a quadratic residue mod \( p^e \). Since \( a \in Q_{p^e} \iff Q_p \) for an odd prime \( p \) (see Theorem 7.13), let us compute the Legendre symbols
\[
\left( \frac{(p + 1)(p - 1)}{p} \right) = \left( \frac{1}{p} \right) \left( -1 \right).
\]
We know that \( 1 \in Q_{p^e} \forall e \), but \(-1 \in Q_{p^e} \) iff \( p = 1 \mod 4 \) for an odd prime \( p \). So we can solve \( y^2 = (p + 1)(p - 1) \mod p^e \) iff \( p = 1 \mod 4 \). The equation \( x + p = y \) can always be solved uniquely. Then, there are 2 solutions if \( p \neq 1 \mod 4 \), and no solutions otherwise.
**Problem 2.** Begin by writing \( a = a_0 \mod p \), where \( 0 \leq a_0 < p \); hence \( a = a_0 + k_1 p \). Iterate this procedure for \( k_1 \) to get \( k_1 = a_1 + k_2 \mod p \), where we similarly choose \( 0 \leq a_1 < p \). Hence, we have

\[
a = a_0 + k_1 p = a_0 + a_1 p + k_2 p^2.
\]

Turning this idea into a inductive hypothesis, assume

\[
a = a_0 + a_1 p + \cdots a_{e-1} p^{e-1} + k_e p^e.
\]

Write, \( k_e = a_e + k_{e+1} p \), and substitute into the above equation to get

\[
a = a_0 + a_1 p + \cdots a_e p^e \mod p^{e+1}.
\]

Since we’ve already tackled the \( e = 1 \) case, we’ve completed the proof of the formula.

The proof that the formula is unique is again by induction. I will do the \( e = 0 \) case: suppose \( a = a_0 \mod p \), and \( a = b_0 \mod p \). Then \( a_0 = b_0 \mod p \), and since \( 0 \leq a_0, b_0 < p, a_0 = b_0 \).

For the final part, let \( k \) be the largest number such that \( p^k | a \). If \( k \geq e \), we can write

\[
a = p^e \mod p^e,
\]

with \( b = 1 \). If \( k < e \), we must have \( a = bp^k \). \( b \) must be coprime to \( p \); for if not, \( b = cp \), and this means that \( p^{k+1} \) divides \( a \). This is contrary to our assumption on \( k \).

**Problem 3.**

**Part (a):** Let \( n = \prod p^e \), and suppose \( a \) is a square mod \( n \). Then, there is an \( x \) s.t. \( x^2 = a \mod n \). It follows from the properties of congruences that \( x^2 = a \mod p^e \) for every prime dividing \( n \).

For the other direction, suppose for each prime \( p \) dividing \( n \), there is an \( x_p \) s.t. \( x_p^2 = a \mod p^e \). The CRT tells us that there is a unique \( x \mod n \) such that \( x = x_p \mod p^e \). Again, by the CRT, there is a unique congruence class mod \( n \) equal to \( a \mod p^e \). Both \( a \) and \( x^2 \) satisfy \( x^2 = a \mod p^e \) for each prime \( p | n \).

Hence, \( x^2 = a \mod n \).

**Part (b):** Let \( a = bp^k \) as in problem 2. The case \( k = e \) is easy, since \( a = 0 \mod p^e \) is always a square. If \( k < e \), we need to show \( a \) is a square if \( k \) is even and \( x^2 = b \mod p^{e-k} \) has a solution. Now, \( a \) is a square if there is an \( x \) s.t. \( x^2 = a \mod p^e \). \( x \) has a decomposition like the one for \( a \) and we can write \( x = cp^r \mod p^e \). Then,

\[
x^2 = c^2 p^{2r} = bp^k \mod p^e \iff 2r = k \text{ and } c^2 = b \mod p^{e-k}.
\]

This is exactly we needed to prove.

We’ve determined that if \( a \) is a square, we can write it as

\[
a = (xp^{k/2})^2 \mod p^e,
\]

where \( x^2 = b \mod p^{e-k} \). Assuming \( b \) is a quadratic residue mod \( n \), let \( N(n) \) be the number of solutions to \( x^2 = b \mod n \). We know that if \( b \) is a quadratic residue mod \( p^e \) and \( p \) is an odd prime, \( N(p^e) = 2 \). If \( p = 2 \), we know that

\[
N(2^e) = \begin{cases} 
1 \text{ if } e = 1, \\
2 \text{ if } e = 2, \\
4 \text{ if } e \geq 3.
\end{cases}
\]
If \( x^2 = b \mod p^{e-k} \) and \( j \) is an integer, any \( y \) of the form
\[
y = (x + j p^{e-k}) p^{k/2}
\]
is a solution to \( y^2 = a \mod p^e \). There are a total of \( p^{k/2} \) distinct \( y \) in \( \mathbb{Z}_{p^e} \), corresponding to \( j = 0, 1, \ldots, p^{k/2} - 1 \). Hence, the total number of square roots of \( a \) is
\[
N(p^{e-k}) p^{k/2}.
\]

Part (c): As in problem 2, let \( x = kp^i \). Then, \( x^2 = k^2 p^{2i} = 0 \mod p^e \) iff \( p^e | k^2 p^{2i} \).

Since \( k \) is coprime to \( p \), it follows that \( 2i \geq e \). Let \( i \) be the smallest integer such that \( 2i \geq e \). Each \( x \) of the form \( a p^i \) is a distinct solution to \( x^2 = 0 \mod p^e \). If \( x = bp^i = ap^i \), we have that \( b = a \mod p^{e-i} \). Hence, there are \( p^{e-i} \) solutions corresponding to \( a = 0, 1, \ldots, p^{e-i} - 1 \).

Remark 1. What we’ve done in Problems 2 and 3 is the following: we know how to find square roots of \( a \mod p^e \) when \( a \in U_{p^e} \); i.e., when \( a \) is coprime to \( p \). This was the theory of quadratic residues. When \( a \) is not coprime to \( p \), \( a \) must be divisible by a prime power \( p^k \), and we proved that we could write
\[
a = bp^k \mod p^e.
\]
The key here is that \( b \) is coprime to \( p \). This meant that we could use our theory of quadratic residues to solve \( x^2 = b \mod p^{e-k} \). The special case \( e = k \) had to be handled separately, and this was done in part (c).

Problem 4.

Part (a): To solve
\[
x^2 + 9x + 27 = 0 \mod 3^e
\]
for all \( e \). Completing the square, we have
\[
y^2 = 54 \mod 3^e,
\]
where \( y = 2x + 9 \). \( 54 = 3^3 \cdot 2 \), and hence, if \( e > 3 \), we have no solutions by problem 3, part b. If \( e = 3 \), \( 54 = 0 \mod 3^e \). Then, using problem 3 part (c), we find \( i = 2 \geq 3/2 \). Hence, there are \( 3^{3-2} = 3 \) solutions. If \( e = 2 \), similarly, there are 3 solutions. If \( e = 1 \), there is one solution.

Part (b): Complete the square to get
\[
(2x + 3)^2 = 45 \mod 3^e.
\]
Note that 45 = \( 3^2 \cdot 5 \). If \( e > 2 \), problem 3 part (b) tells us that 45 is a square if we can solve \( x^2 = 5 \mod 3^{e-2} \). That is, we want to determine whether 5 \( \in Q_{3^{e-2}} \) and so we compute the Legendre symbol,
\[
\left( \frac{5}{3} \right) = \left( \frac{3}{5} \right) = -1.
\]
Hence, 5 is not a square root, and we have no solutions for \( e > 2 \). For \( e = 1 \), we have 1 square root, and \( e = 2 \), we have 3 square roots as in part (a). Each of these square roots corresponds to a solution to the quadratic.

Part (c): Complete the square and get:
\[
y^2 = 4 \cdot 3^2 \mod 3^e
\]
where \( y = 2x + 3 \). For \( e > 2 \), we can always solve \( x^2 = 4 \mod 3^{e-2} \), since 4 is obviously a quadratic residue. There are 6 square roots mod \( 3^e \), and each gives
a solution $x$ to the quadratic. For $e = 1$ and $e = 2$, there are 1 and 3 solutions respectively.